

STEPTOE & JOHNSON LLP

ATTORNEYS AT LAW

1330 CONNECTICUT AVENUE, N.W.
WASHINGTON, D.C. 20036-1795

PHOENIX, ARIZONA
TWO RENAISSANCE SQUARE

TELEPHONE: (602) 257-5200
FACSIMILE: (602) 257-5299

PETER LICHTENBAUM
(202) 429-6259

(202) 429-3000

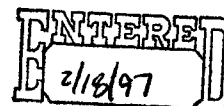
FACSIMILE: (202) 429-3902

TELEX: 89-2503

STEPTOE & JOHNSON INTERNATIONAL
AFFILIATE IN MOSCOW, RUSSIA

TELEPHONE: (011-7-501) 258-5250
FACSIMILE: (011-7-501) 258-5251

February 14, 1997



Ms. Nancy Crowe
Regulatory Policy Division
Bureau of Export Administration
Department of Commerce
14th Street and Pennsylvania Ave., N.W.
Room 2705
Washington, D.C. 20230

Dear Ms. Crowe:

The following comments are submitted on behalf of VISA USA Inc. and Visa International (collectively "Visa") in response to the Commerce Department's request for comments on its interim-final encryption regulations. See 61 Fed. Reg. 68572 (Dec. 30, 1996).

As way of background, Visa is a membership organization representing almost 21 thousand financial institutions on a worldwide basis. There are more than 525 million Visa cards in circulation among consumers globally, accepted at more than 12 million merchant locations and 282,000 automated teller machines worldwide. Visa provides authorization, clearing and settlement services to member financial institutions in support of a wide range of card-based products and services. Visa members reported total sales of \$886.4 billion for the four quarters ending June 30, 1996.

To support the volume of transactions that are processed by the retail payment network, Visa and its member banks have a vital interest in promoting a secure electronic financial system. Moreover, VISA USA and its member banks have adopted significant mechanisms to ensure the integrity of

Ms. Nancy Crowe
February 14, 1997
Page 2

electronic transactions. Visa and its member banks play a leading role in defining measures needed to ensure the safe and sound operation of retail payment mechanisms. Visa has implemented a comprehensive system of controls to provide member banks with the assurance they need for the security, integrity and reliability of Visa payment systems.

Because of Visa's significant role in establishing secure retail payment mechanisms, Visa believes it is essential for U.S. export controls on encryption for financial uses to develop in a way that is consistent with the Visa network's established security procedures.

Therefore, Visa welcomed the statement by Vice President Gore, when he announced the Administration's new encryption initiative in October 1996, that exports for certain financial uses would continue to receive special treatment. The Vice President's statement appropriately recognized, consistent with past State Department licensing policy, that a flexible licensing approach is essential in order to allow the financial industry to build a secure electronic international financial system. In addition, Comptroller of the Currency Eugene Ludwig has said that "the market will decide" the role of electronic payments systems, and that "inappropriate and excessive regulation can badly damage the promise that these new technologies hold." Similarly, then-Federal Reserve Board Vice Chairman Alan S. Blinder said that the Fed "has not the slightest desire to inhibit the evolution of this emerging industry by regulation, nor to constrain its growth."

Accordingly, Visa hopes that the Administration will ensure that the final encryption regulations appropriately recognize the special circumstances of financial sector end-uses. Visa recognizes and appreciates that the previous "money or banking" exception for certain financial applications that existed under State Department controls has been carried over in the interim regulations. However, the "money or banking" exception has been narrowed by deleting the reference to "equipment for the encryption of interbanking transactions." Visa hopes that this apparent oversight will be corrected given its potentially harmful effect on the electronic payments system.

Visa's understanding is that the Administration does not intend to impose greater restrictions on encryption exports for financial end-uses than existed under the State Department controls. However, the regulations do not clearly state the Administration's policy regarding financial end-uses. The lack of transparency in the interim regulations may create uncertainty in the financial industry about the Administration's policy. Therefore, Visa suggests that the final regulations clarify the rules that will apply for financial end-uses.

Visa's primary concern is that these rules should not require products using 56-bit DES encryption or stronger encryption ("strong encryption") for financial end-uses to implement key recovery. Visa is concerned that requiring products using strong encryption for financial end-uses to implement key recovery will be expensive and unproductive, because this approach would not take into account the established private sector security procedures.

First, there is no demand from Visa member banks for key recovery in this context, because the data is not stored in an encrypted form. In the Visa payment system, communications between banks or between banks and their customers are generally encrypted only during the short period from the initial transmission until receipt. Because the data is stored securely in a clear-text form, there is no reason for a customer to recover its key.

Second, key recovery is not necessary in the context of financial communications. After decrypting the transmission, financial institutions verify the authenticity and integrity of the sender and data and then store the data securely in a clear-text form. Therefore, financial institutions can make the clear-text data available pursuant to legal process without storing or archiving user keys.

Third, requiring key recovery for real-time communications data may not be technically feasible, since banks would need to recover thousands or millions of session keys generated daily by employees, customers and others. Even if

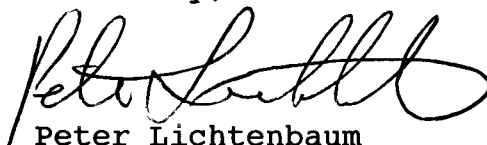
Ms. Nancy Crowe
February 14, 1997
Page 4

feasible, such a requirement would be very expensive for Visa's member banks to implement. Moreover, storage and recovery of session keys is inconsistent with the security architecture of session keys, i.e., erasure following use.

As a result, Visa is concerned that the existing regulations may not spur the adoption of key recovery encryption, but may instead restrict U.S. financial sector companies' ability to lead the development of a secure international electronic commerce infrastructure. Given the vital importance of securing financial transactions, the Administration should recognize the special status of encryption exports for financial end-uses, such as home banking and credit card purchases, and should clarify this approach in the final regulations. By doing so, the Administration will ensure that the Vice President's commitment is implemented and will enable U.S. companies to lead the way in building a secure framework for international electronic commerce.

Visa appreciates the opportunity to submit comments on this important issue.

Sincerely,

A handwritten signature in black ink, appearing to read "Peter Lichtenbaum", with a stylized, cursive script.

Peter Lichtenbaum